(d) *Organizational.* The Offices of Security in State, AID, and USIA are responsible for physical, procedural, and personnel security in their respective agencies. In the Department of State, the Office of Communications (COMSEC) is responsible for communications security.

§9.4 Classification.

(a) When there is reasonable doubt about the need to classify information, the information shall be safeguarded as if it were ''Confidential'' pending a determination about its classification by an original classification authority. When there is reasonable doubt about the appropriate classification level, the information shall be safeguarded at the higher level pending the determination of its classification level by an original classification authority. Determinations hereunder shall be made within 30 days.

(b) Information may not be classified unless its disclosure reasonably could be expected to cause damage to the national security. Information may not be classified to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

(c) The President or an agency head or official designated under section 1.2 (a)(2), 1.2 (b)(1), or 1.2 (c)(1) of the Order may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security, and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of ISOO.

(d) It is permitted to classify or reclassify information after an agency has received a request for it under the Freedom of Information Act or the Privacy Act, or the mandatory review provisions of the Order, provided that such classification meets the requirements of the Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior official, or an official with original Top Secret classification authority. Every effort should be made to classify properly at the time of origin. When a determination is made that a document requires classification or reclassification, however, all holders of the document should be notified and, in the Department of State, a copy of the classification or reclassification memorandum should be sent to the Foreign Affairs Information Management Center (FAIM). In addition, if the classification or reclassification was done in any office other than the DAS/CDC, that office should send a copy of the pertinent memorandum to the CDC.

(e) For the Department of State, these functions will be performed by the DAS/CDC.

(f) For AID, the function will be performed by the Administrator.

(g) For USIA, the function will be performed by the Director of Public Liaison.

(h) Information classified in accordance with these regulations shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

§9.5 Classification designations.

(a) Only three (3) designations of classification are authorized: ''Top Secret,'' ''Secret,'' and ''Confidential.''

(1) *Top Secret.* Information may be classified ''Top Secret'' if its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. This classification should be used with the utmost restraint. Examples of ''exceptionally grave damage'' include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

(2) *Secret.* Information may be classified ''Secret'' if its unauthorized disclosure could reasonably be expected to

cause serious damage to the national security. This classification should be used sparingly. Examples of ''serious damage'' include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

(3) *Confidential.* Information may be classified ''Confidential'' if its unauthorized disclosure could reasonably be expected to cause damage to the national security. Except as otherwise provided by statute, no other terms shall be used to identify classified information. Terms or phrases such as ''For Official Use Only'' or ''Limited Official Use'' shall not be used to identify national security information. No other term or phrase shall be used in conjunction with these national security information designations, such as ''Secret Sensitive'' or ''Agency Confidential'' to identify national security information.

(b) *Foreign government information.* If classified by the foreign government, the information shall either retain its original classification or be assigned a U.S. classification designation which will ensure a degree of protection at least equivalent to that required by the entity that furnished the information. If not given a specific classification by the foreign government, the information will be assigned an appropriate classification dependent on the sensitivity of the subject matter and the degree of damage its unauthorized disclosure could reasonably be expected to cause to the national security. Classification designations assigned by the U.S. agency shall be marked on the foreign government information in accordance with the provisions of §9.12.

§9.6 Requirements for classification.

With the exception of the Atomic Energy Act of 1954, as amended, these regulations are the only basis for classifying information in the agencies named herein. To be eligible for classification, information must meet the two following requirements:

(a) First, it must deal with one of the following criteria:

(1) Military plans, weapons, or operations;

(2) The vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

(3) Foreign government information;

(4) Intelligence activities (including special activities), or intelligence sources or methods;

(5) Foreign relations or foreign activities of the United States;

(6) Scientific, technological, or economic matters relating to the national security;

(7) U.S. Government programs for safeguarding nuclear materials or facilities;

(8) Cryptology;

(9) Confidential sources; or

(10) Other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. In the Department of State, the DAS/CDC, as the senior official, shall recommend such other categories of information to the Secretary. Any determination made under this subsection shall be reported promptly to the Director of ISOO.

(b) Second, an official with original classification authority must determine that the unauthorized disclosure of the information, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security. Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

(c) Certain information which would otherwise be unclassified may require classification when combined or associated with other classified or unclassified information. Classification on this basis shall be supported by a written explanation that, at a minimum, shall be maintained with the file or record copy of the information.